Exhibit 122

Learn more about ES&S.; For answers to frequently asked questions, click here >>   **FAQs**
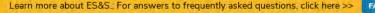
ELECTION Systems & Software

COVID-19 Resources | 877-377-8683 | myES&S Portal | 🔍 Search

Voter Resources   What We Do ⌄   Products ⌄   Security   Resources ⌄

RESOURCES

Getting the facts straight about elections.

Every election reinforces the importance of voting as the foundation of America's democracy. Nothing is more important to ES&S than maintaining the integrity of the voting process. By understanding the real risks to elections, we strengthen our ability to protect democracy.

Let's get the facts straight.

Who provides ES&S with its software and where is it developed?

ES&S designs and builds its own tabulation software, which is developed and compiled exclusively in the USA.

Do ES&S voting systems use Smartmatic software?

No. ES&S designs and builds its own software from the ground up. All ES&S software is developed and compiled exclusively in the USA.

Is ES&S affiliated with any other companies which produce voting systems?

ES&S has no financial or ownership ties to any other voting system manufacturers.

Do ES&S voting systems use proportional, weighted or fractional voting?

No. ES&S tabulation firmware does not support proportional, weighted or fractional voting.

Have America's voting machines been hacked in the past?

While the threats are very real, there's no evidence that any vote in a U.S. election has ever been compromised by a cybersecurity breach. To date, the totality of security measures — such as tamper-resistant seals, audits, voting machines which do not connect to the internet (see modem note below), along with more advanced technology found in newer equipment — provides for an environment that would be difficult to compromise. As threats become more sophisticated, so must voting machines and the nation's entire voting infrastructure.

Click here to download CIS's best practices for securing connected, non-voting election technology.

Why are modems allowed to transmit results?

Document title: FAQs - Election Systems & Software
Capture URL: https://web.archive.org/web/20210102201534/https://www.essvote.com/faqs/
Capture timestamp (UTC): Fri, 08 Oct 2021 14:37:59 GMT

Click here to download CIS's best practices for securing connected, non-voting election technology.

Why are modems allowed to transmit results?

In a few states it is a legal practice to use cellular modems to transmit unofficial election results after the polls are officially closed and all voting has ended. ES&S uses mobile private network connectivity, industry best practices, and numerous security safeguards to protect the transfer of these unofficial election night results. Final official results are physically uploaded at election headquarters prior to final certification. The physical ballots and printed results tapes are always protected.

Can we trust ES&S voting machines?

Voting machines provided by ES&S are certified by the federal Elections Assistance Commission and undergo robust testing for accuracy, reliability, usability and security. There is no evidence of a voting machine being compromised by a cybersecurity incident in an election. Voting machines are used and deployed in a decentralized manner across the nation's 10,000 voting jurisdictions. This decentralization greatly diminishes the chance or impact of a large-scale attack. While there is no evidence of any hacking of any voting machine currently in use as it is used in an election, as threats become more sophisticated, so must voting machines and the nation's entire voting infrastructure.

Can voting machines be hacked?

Voting machines have been hacked at staged demonstrations and in laboratories, but these environments do not reflect an actual election scenario where multiple layers of physical and cyber security are always in place. These measures include pre-election testing, locks, restricted access, tamper-resistant seals, chain-of-custody protocols, and voting machines which are locked down to ensure limited access, along with more advanced technology found in newer equipment.

If I have a key that can open an ES&S machine lock, does that mean I can easily get into and hack the machine?

No. Doors and locks are just one of the deterrents to tampering with a voting machine. During an election, there are many security measures beyond doors and locks, including tamper-resistant, serial-numbered seals to ensure security. If a seal is broken, it can't be replaced without detection. We also have multiple layers of encrypted security on the data, including unique encryption keys for every election. This ensures that all our voting machines will only accept USB flash drives programmed for that election and prevents tampering by unauthorized agents.

When I cast my ballot, does it matter whether I put my paper ballot face-up or face-down in the scanner?

No. Thanks to dual-scanning technology, ES&S tabulation machines – the DS200, DS450 and DS850 – can read ballots no matter which direction they are placed in machine.

Are older voting machines secure?

Older equipment is protected by multiple layers of physical and technical security including tamper-resistant seals and controlled access. That said, newer equipment has more advanced technology and is more secure.

Are elections systems providers being transparent?

ES&S values transparency and works closely with all levels of the U.S. government, academia and other experts to ensure the integrity of America's voting. ES&S has invited and welcomed numerous experts and government officials, including critics, to see its operations first hand and to discuss improvements. ES&S actively collaborates with the U.S. Department of Homeland Security, has all its equipment certified through the U.S. Elections Assistance Commission, and willingly takes part in many other collaborations with groups and individuals interested in protecting America's voting system.

Does ES&S use independent testing of its voting equipment?

system.

Does ES&S use independent testing of its voting equipment?

Yes, in multiple ways. ES&S voluntarily adheres to the Federal Testing Program conducted by the Election Assistance Commission (EAC), a federal agency created by the Bi-Partisan Help America Vote Act of 2002. Under the EAC, ES&S submits all its systems to Voting System Test Laboratories accredited by NIST. These labs perform tests in accordance with the federal voting system standards. Layered upon the reviews conducted under the Federal Test Program, several states also engage independent firms to audit the security of voting machines as part of the certification examination process in their states. In addition, over the past year, ES&S engaged with cybersecurity firms to conduct independent third-party reviews, including penetration testing and source code reviews. And in cooperation with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), ES&S also submitted its end-to-end voting configuration for testing by the **Idaho National Laboratory (INL)**, the nation's leading center for research and development in energy, national security, science and environment.

Does ES&S support security enhancements to the nation's election infrastructure?

ES&S fully supports paper-based voting technology coupled with post-election audits. ES&S supports the creation or adoption of industry standards and guidelines which further strengthen the nation's critical election infrastructure. ES&S has taken multiple steps to bolster security.

Are you aware of any data breaches or other cybersecurity incidents in which an attacker gained unauthorized access to your internal systems, corporate data or customer data?

No, we are not aware of any cybersecurity incidents in which an attacker gained unauthorized access to ES&S internal systems or corporate data.

Do you have a process in place to receive and respond to unsolicited vulnerability reports from cybersecurity researchers and other third parties?

Yes, ES&S utilizes its internal corporate information security staff to receive, evaluate and act upon, as necessary, unsolicited vulnerability reports from cybersecurity researchers and other third parties. In addition, ES&S maintains **a link on its website** for the purpose of receiving and responding to reports and/or inquiries related to security.

How does ES&S protect its hardware and software supply chain?

As standard practice, each release undergoes extensive security testing and ES&S provides a complete set of software components to the voting systems testing labs (VSTL) for review. ES&S also conducts thorough security reviews of our entire supply chain to ensure that every component is trusted, tested and free of malware. Every single item and manufacturer are approved and under engineering revision control. That's the advantage of an ES&S purpose-built system versus one with components bought off the shelf.

Click here to learn more about the supply chain and manufacturing of voting systems.

I understand ES&S ballot marking systems use barcodes. Can barcodes really be trusted?

Barcodes are a trusted, tested, universal technology used in a variety of ways across many different industries to improve safety, accuracy, speed and efficiency. DMVs, pharmacies, hospitals, banks and food manufacturers all use barcodes. Vote counting machines (called tabulators) read barcodes in the same way they read the oval positions on a paper ballot—so a summary card with barcodes contains the same data as on a hand-marked ballot. Because barcodes offer a reliable way to accurately read information, the technology all but eliminates the possibility of human error (e.g. poorly marked ballots, misinterpretation of voter intent). Displayed along with human-readable text, summary cards with barcodes are fully auditable.

Click here to read more about how barcodes are read.

Click here to watch a video about how ballots are read.

Does ES&S support post-election audits?

Click here to watch a video about how ballots are read.

Does ES&S support post-election audits?

ES&S is a strong supporter of post-election audits – a way for election officials to verify that votes were counted accurately. Post-election auditing is conducted by election officials. ES&S voting systems provide audit details (logs, cast vote records, reports, etc.) which election officials utilize for this purpose.

Does ES&S support the use of paper in elections?

ES&S views paper records as critical for auditing. ES&S decided in 2018 to no longer sell paperless voting machines as the primary voting device in a jurisdiction because it is difficult to perform a meaningful audit without a paper record of each voter's selections. Using a physical paper record sets the stage for all jurisdictions to perform statistically valid post-election audits.

I understand that ES&S election software operates on Windows. What does that mean for election security?

Election systems are hardened, meaning that the computer that runs Windows is locked down with allowed access only to the functions required to conduct an election. Unused ports are blocked, and unnecessary services are removed. This hardening means that work stations running on Windows platforms are protected from the types of risks more commonly associated with mainstream technologies. For systems that currently use Windows 7, ES&S and Microsoft will provide ongoing support for that software until jurisdictions can upgrade to our latest versions which now incorporate Windows 10.

Do any of your systems currently deployed have any kind of remote access capability, and, if so, how many?

No ES&S product or system has remote access capability; ES&S does not provide this capability.

ES&S systems in the past included remote-access capability—why?

More than a decade ago, ES&S, along with others in this industry and many other industries, provided software upon customer request for customer workstations—not voting machines—for troubleshooting purposes. While no known issues arose with this practice, ES&S has not provided this capability since 2007 and never provided it for voting machines.

How big is ES&S?

ES&S serves about 1,668 county-level jurisdictions across the U.S.

Who owns ES&S?

ES&S is 100% American-owned by McCarthy Group and individual members of ES&S management. McCarthy Group originally partnered with the founders of ES&S in 1987 and for more than thirty years has supported ES&S as it has grown into the industry leader with solutions for each step of an election. ES&S' stable partnership with McCarthy Group has enabled continuous investment in research and development, resulting in new and improved voting technology built with the highest standards of security that help election officials run secure and successful elections.

Why trust a private company with our nation's elections?

The elections infrastructure, like the nation's power grid, is made up of public and private partnerships. As DHS says in describing critical infrastructure, there is a shared responsibility among multiple stakeholders because neither the government nor the private sector alone has the knowledge, authority, or resources to do it alone.

ES&S systems in the past included remote-access capability—why?

More than a decade ago, ES&S, along with others in this industry and many other industries, provided software upon customer request for customer workstations—not voting machines—for troubleshooting purposes. While no known issues arose with this practice, ES&S has not provided this capability since 2007 and never provided it for voting machines.

How big is ES&S?

ES&S serves about 1,668 county-level jurisdictions across the U.S.

Who owns ES&S?

ES&S is 100% American-owned by McCarthy Group and individual members of ES&S management. McCarthy Group originally partnered with the founders of ES&S in 1987 and for more than thirty years has supported ES&S as it has grown into the industry leader with solutions for each step of an election. ES&S' stable partnership with McCarthy Group has enabled continuous investment in research and development, resulting in new and improved voting technology built with the highest standards of security that help election officials run secure and successful elections.

Why trust a private company with our nation's elections?

The elections infrastructure, like the nation's power grid, is made up of public and private partnerships. As DHS says in describing critical infrastructure, there is a shared responsibility among multiple stakeholders because neither the government nor the private sector alone has the knowledge, authority, or resources to do it alone.

ELECTION Systems & Software

ES&S Headquarters 11208 John Galt Blvd Omaha, NE 68137

EXPLORE

Products

How We Help

Find Your Rep

Blog

Case Studies

WHO WE ARE

About

Management Team

Contact

Media Resources

Careers

Intellectual Property

SOCIAL

f   Facebook

🐦   Twitter

in   LinkedIn